2008-2009

Information Security Strategic Plan

OFFICE OF THE CHIEF INFORMATION OFFICER

Information Technologies Department

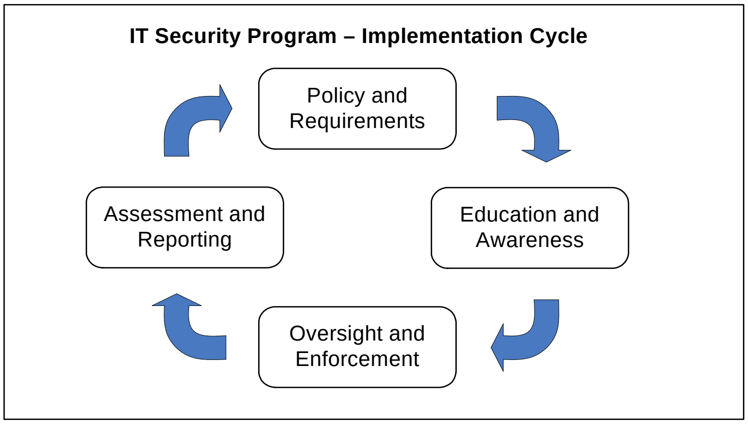
Information Security Office

Executive Summary

In December 2006, El Dorado County officially assigned roles and responsibilities of a Chief Information Security Officer (CISO) for the purpose of building an Information Security Program for the county.

This report summarizes El Dorado County's strategic plan for launching an Information Security Program. The plan is represented as a set of goals for Program implementation and oversight.

It is important to note that establishing an Information Security Program is not a one-time event, but an ongoing venture that follows a cyclical process. The implementation phases (see below) are not cleanly separated processes, but instead represent a flow of activities that yield an ever maturing Program. The implementation cycle involves establishing information security requirements, educating people about their responsibilities under those requirements, building governance structures to ensure Program compliance, and monitoring and reporting of progress.


IT Security Program – Implementation Cycle

Mission

The Information Security Office is dedicated to providing superior information security services to all employees and citizens of El Dorado County ensuring the confidentiality, integrity and availability of data.

Vision

The Vision of the Information Security Office is to become a recognized leader in protecting El Dorado County's information desired by citizens, employees and organizations, while maximizing access in a safe and secure manner.

Strategic Goals for Program Implementation

The Information Security Office has established six goals to establish formal information security management and governance processes.

- ***Develop, Approve, and Promote a Comprehensive Information Security Policy Suite***
- ***Ensure All Employees are Aware of their Information Security Responsibilities***
- ***Establish Oversight Authority for Information Security for Each Department***
- ***Establish a Process for Regular Progress Reporting to Executive Leadership***
- ***Implement Controls Enabling Countywide Compliance of Mandated Regulations***
- ***Implement and Enhance Business Continuity and Disaster Recovery Programs***

These goals and accompanying strategic objectives provide the priorities for Information Security investments of effort and resources over the next two years. The following summarizes the strategic objectives to attain these goals.

Goal 1: Develop, Approve, and Promote a Comprehensive Information Security Policy Suite
In collaboration with all appropriate County Security representatives, yet to be determined, the CISO will lead efforts to develop, approve, and launch a suite of enterprise information security policies, based on the ISO 27002 code of best practices for information security. These policies will formally establish the El Dorado County Information Security Program and set forth employee responsibility for information protection.

Goal 2: Ensure All Employees are Aware of their Information Security Responsibilities
Require all employees to participate in information security awareness courses, which serve to inform employees of their responsibilities for protecting the information in their care. To complement employee awareness of responsibility, a training program will be developed to ensure county employees have the knowledge needed to carry out those responsibilities within their respective depts.

Goal 3: Establish Oversight Authority for Information Security for Each Department
Designate a person at each department with information security oversight authority for all Information Security operations at each respective department location. Such a person would have the authority to enforce the requirements of county and departmental policies for information security.

Goal 4: Establish a Process for Regular Progress Reporting to Executive Leadership
The CISO shall establish a regular schedule for reporting of Information Security Program development progress to the Chief Information Officer CIO. The CISO will also review enterprise-wide and departmental assessments and progress reports and deliver management briefings on a regular basis to the Governance Body, Executive Leadership and Management.

Goal 5: Implement Controls Enabling Countywide Compliance of Mandated Regulations
Perform an initial gap analysis and implement minimum security requirements and technical controls that address the management, operational, and technical aspects of protecting the confidentiality, integrity and availability of county data and information systems in accordance with various federal, state and local regulations.

Goal 6: Implement and Enhance Business Continuity and Disaster Recovery Programs
The county has established and continues to build and enhance the Continuity of Government Operations (COOP) Business Continuity Program including business resumption planning for various departments and business units. The CISO shall build a Disaster Recovery Program for the protection and recoverability of critical systems, network services, applications and related data.

Strategic Plan Overview

PURPOSE

The purpose of the Information Security Strategic Plan is to provide the direction desired to implement an Information Security Program. The Plan provides a framework of goals and objectives essential to support the county's commitment to the confidentiality, integrity and availability.

CHALLENGES TO STRATEGIC PLANNING

Developing and implementing a successful strategic plan to properly protect the county's vast information systems resources and associated data involves an enormous set of challenges. The challenges include:

- Significant resource, personnel, and related budget issues
- Governance issues
- A dynamic regulatory environment
- The sheer volume of computer systems and the separate services that they are designed to provide
- The volume of data involved
- Numerous, different operating system types and customized configurations
- Vulnerabilities with emerging computer and network technologies that cannot be easily resolved
- A constant, rapidly expanding spectrum of threats to computing systems and networks
- The size and diversity of El Dorado County departmental workforce and their essential services they provide to the citizens

This strategic plan proposes to reduce the incidents of intrusions, misuse of its computing resources, and inappropriate access to data. Since there are many departments and business units within El Dorado County that currently do not have budgeted resources for Information Technology, much less specifically for security, the resources and the necessary expertise to support security efforts will need to be allocated.

Goal 1: Develop, Approve, and Promote a Comprehensive Information Security Policy Suite
El Dorado County must have in place appropriate policies and best practices guidelines to ensure a safe, compliant, and properly risk managed computing and network environment. In addition to formal policy, specific guidelines and recommended procedures for the El Dorado County workforce shall be published to help address a broad range of administrative concerns including but not limited to:

- Updating and enforcing Acceptable Use Policies contained within “El Dorado County Computer and Network Resource Usage Policies and Standards Guide – General Use”
- Information access controls including specifics regarding appropriate access authorization to systems and data
- The receipt, storage, processing, and distribution of sensitive information
- Security review and testing of hardware and software installations, and maintenance of existing systems
- General data protection practices such as security violation reporting, sanctions for violations, data backup and or electronic media control measures
- Employee termination responsibilities and the removal of data accessibility
- Assessing and managing risk

Goal 2: Ensure All Employees are Aware of their Information Security Responsibilities

A countywide Security Awareness, Training and Education Program must be developed and implemented based on current resources that are available. Education and training is one of the most cost-effective security measures an organization can adopt.

The program must be flexible in content, message, and design to accommodate multiple targeted audiences: Board of Supervisors, directors, management, system administrators, network administrators, employees and departmental specific content (HIPAA). The content and message must support the strategic message that everyone is responsible to do their part to protect the county’s information systems and information assets. Steps to create the program include:

- Perform a Gap Analysis identifying current environment and knowledge base
- Establish priorities (availability of material/resources, personnel resources)
- Determining how to fund the program
- Developing awareness material (email advisories, web pages, newsletters)
- Selecting awareness topics (Acceptable Use Policies)
- Developing training material based on business function (administrator, manager, user, developer)
- Techniques for delivering training material (web, computer-based training, instructor-led)

Goal 3: Establish Oversight Authority for Information Security for Each Department

El Dorado County must ensure that an appropriate organizational structure exists to provide oversight and governance for security services, related planning, and associated risk management practices. Establishing oversight responsibilities within the county will consist of formal oversight (Governance) and informal oversight (Departmental representatives).

The formal organizational component must be sponsored and support by the county executive leadership to give it the authority it needs to succeed and meet mandated regulations and other requirements.

Formal oversight responsibilities may include, but are not limited to:

- Developing, publishing, and maintaining comprehensive countywide information systems security plans, policy, procedures, and guidelines
- Acting as liaison for disputes, requests for exceptions, and complaints regarding countywide information systems security practices and related issues
- Acting as the primary control point during serious security incidents
- Providing county executive leadership recommendations as required regarding risk management issues related to information systems technologies

The informal organizational component must be supported and enforced by each respective department director to implement countywide appropriate policy and guidelines established by the governance body and to meet mandated state and federal regulations.

Informal oversight responsibilities may include, but not limited to:

- Ensuring respective departmental employees are following approved policy and guidelines
- Providing the technical resources to ensure that security safeguards are implemented according to policy or guidelines
- Designating an Information Security Officer for respective department
- Reporting to Chief Information Security Officer on measurements or metrics established by the governance body

In general, finding enough organizational resources to properly support security functions will always be problematic. This is especially true within a county government. Wherever possible, the governance body should use its designated responsibilities to promote and support the allocation of staff resources and budget to support security efforts. In addition, the governance body should use its considerable expertise and strategic perspectives to prioritize projects and efforts to ensure the best use of resources.

Goal 4: Establish a Process for Regular Progress Reporting to Executive Leadership

Communication must be horizontal and vertical in nature. In El Dorado County, the CISO reports directly to the Chief Information Officer (CIO). Most organizations are utilizing this relationship. The advantage of this reporting model is there is a strong assumption that the CIO has the understanding of the technical issues and typically has the authority with senior management to make the desired changes. It is also beneficial because the CISO has to spend a good deal of time interacting with the rest of the Information Technologies department, which builds the appropriate awareness of activities and issues. Communication must also occur with Board of Supervisors, Chief Administration Office, Human Resources, Risk Management, Privacy/Compliance Officer, Health departments falling under the HIPAA umbrella, and County Counsel.

Goal 5: Implement Controls Enabling Countywide Compliance of Mandated Regulations

Specific to information systems that maintain sensitive information and that are subject to mandatory regulations, El Dorado County must ensure information systems access controls provide for the assurance that only persons with a need can access specific information. This means that appropriate access is given only to that information an individual requires in order to perform their job. Types of access controls can include mandatory access controls, discretionary access controls, time-of-day and classification.

The threat of computer viruses is well documented and understood. Everyone is vulnerable even with the latest virus protection software installed, updated, and operational. The county, like every other organization, must work constantly to protect itself and continue to allocate resources to respond to virus incidents.

Mandated control measures the county is required to meet include, but are not limited to:

- Assisting HIPAA departments in establishing their respective security policies
- Incorporating Device and Media Disposal
- Minimizing Media Re-Use
- Enforcing Password Complexity requirements
- Enforcing Password changes
- Perform logging and auditing functions
- Implement Email Encryption functionality
- Implement laptop encryption methods
- Implement removable media encryption methods

Goal 6: Implement and Enhance Business Continuity and Disaster Recovery Programs

There are many risks that may threaten and disrupt El Dorado County's business processes. These risks include fires, floods, earthquakes, risks from terrorism and telecommunications failures, theft, and employee sabotage.

Business Continuity is a comprehensive process to ensure the continuation and improvement of business in the face of whatever challenges the county may face. Continuity planning requires many processes be used together to create a complete continuity plan. The plan must be maintained and updated as business processes change and tested. Business Continuity Plans enable the county to understand the risks and exposures that it faces and provide a clear understanding of what is needed to ensure survival through preventative measures. Elements that go into Business Continuity Planning include:

- Risk Evaluation and Control
- Business Impact Analysis
- Developing Business Continuity Strategies
- Emergency Response and Operations
- Awareness and Training
- Maintaining and Exercising Business Continuity Plans

Disaster Recovery Planning addresses the recovery planning needs of the county's IT infrastructures, including centralized and decentralized IT capabilities, as well as voice and data communications and network support services. Recovery of IT alone does not ensure survival of the enterprise following a serious disruption or disaster. Speedy recovery of all the components of IT is useful only if the county's business units are able to continue functioning, at some level, throughout the event. The county must in a position to continue to communicate with the public, organizations or patients, key business partners, vendors, employees, and employees' families,. The county must also be able to receive and enter orders, provide services, collect and book revenue, account for assets, etc.
The customer must work with the IT department to define and agree upon functional and technical requirements for IT recovery strategies.

A number of considerations need to be considered including:

- Systems Hardware Resources
- Systems Data Storage Requirements
- Unique (ie., nonstandard) Hardware Resources
- Distributed systems (e.g., workstations, intranets, etc.)
- File Backup capability (disk-to-disk, disk-to-tape, off-site storage, data mirroring, etc.)
- File recovery capability (from disk, from tape on-site and off-site)
- Cold Sites, Warm Sites, Hot Sites, Mobile Sites, Virtual Business Partners, etc.